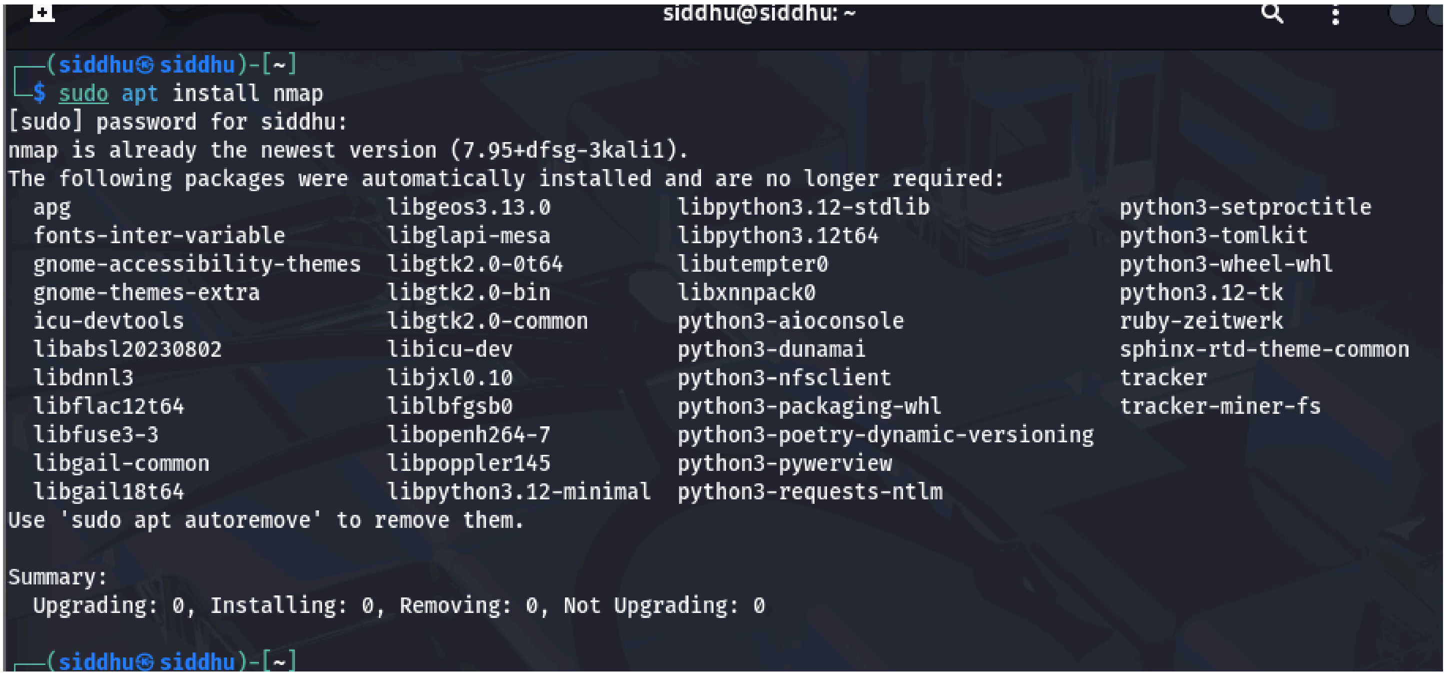
ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-1:

1.Install Nmap from official website



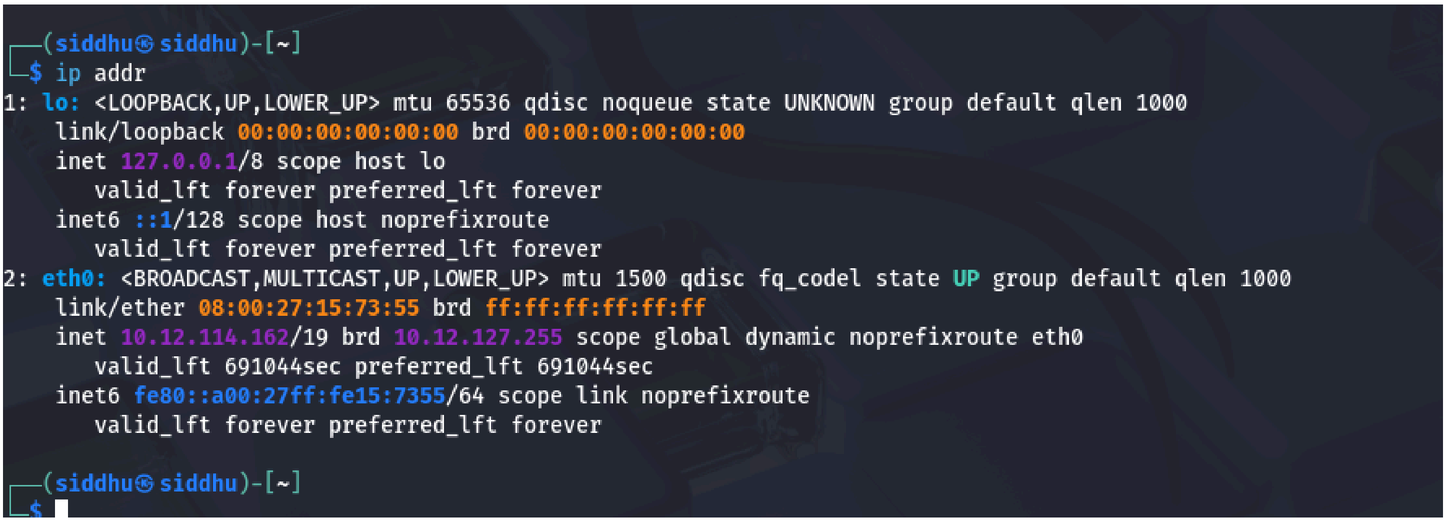
```
┌──(siddhu㉿siddhu)-[~]
└─$ sudo apt install nmap
[sudo] password for siddhu:
nmap is already the newest version (7.95+dfsg-3kali1).
The following packages were automatically installed and are no longer required:
  apg                         libgeos3.13.0          libpython3.12-stdlib               python3-setproctitle
  fonts-inter-variable        libglapi-mesa          libpython3.12t64                   python3-tomlkit
  gnome-accessibility-themes  libgtk2.0-0t64         libutempter0                       python3-wheel-whl
  gnome-themes-extra          libgtk2.0-bin          libxnnpack0                        python3.12-tk
  icu-devtools                libgtk2.0-common       python3-aioconsole                 ruby-zeitwerk
  libabsl20230802             libicu-dev             python3-dunamai                    sphinx-rtd-theme-common
  libdnnl3                    libjxl0.10             python3-nfsclient                  tracker
  libflac12t64                liblbfgsb0             python3-packaging-whl              tracker-miner-fs
  libfuse3-3                  libopenh264-7          python3-poetry-dynamic-versioning
  libgail-common              libpoppler145          python3-pywerview
  libgail18t64                libpython3.12-minimal  python3-requests-ntlm
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(siddhu㉿siddhu)-[~]
```

2.Find your local IP range

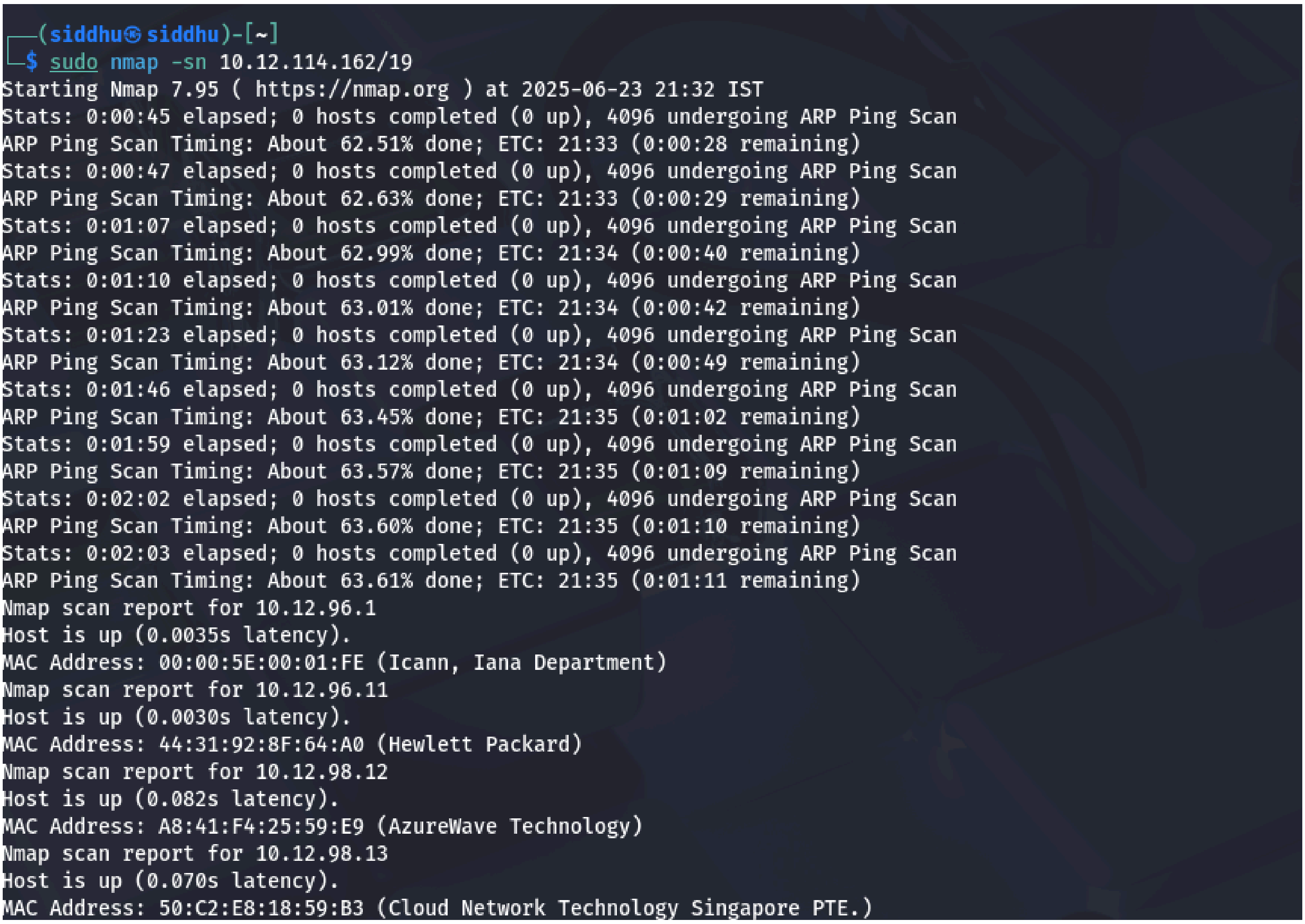
by using if addr



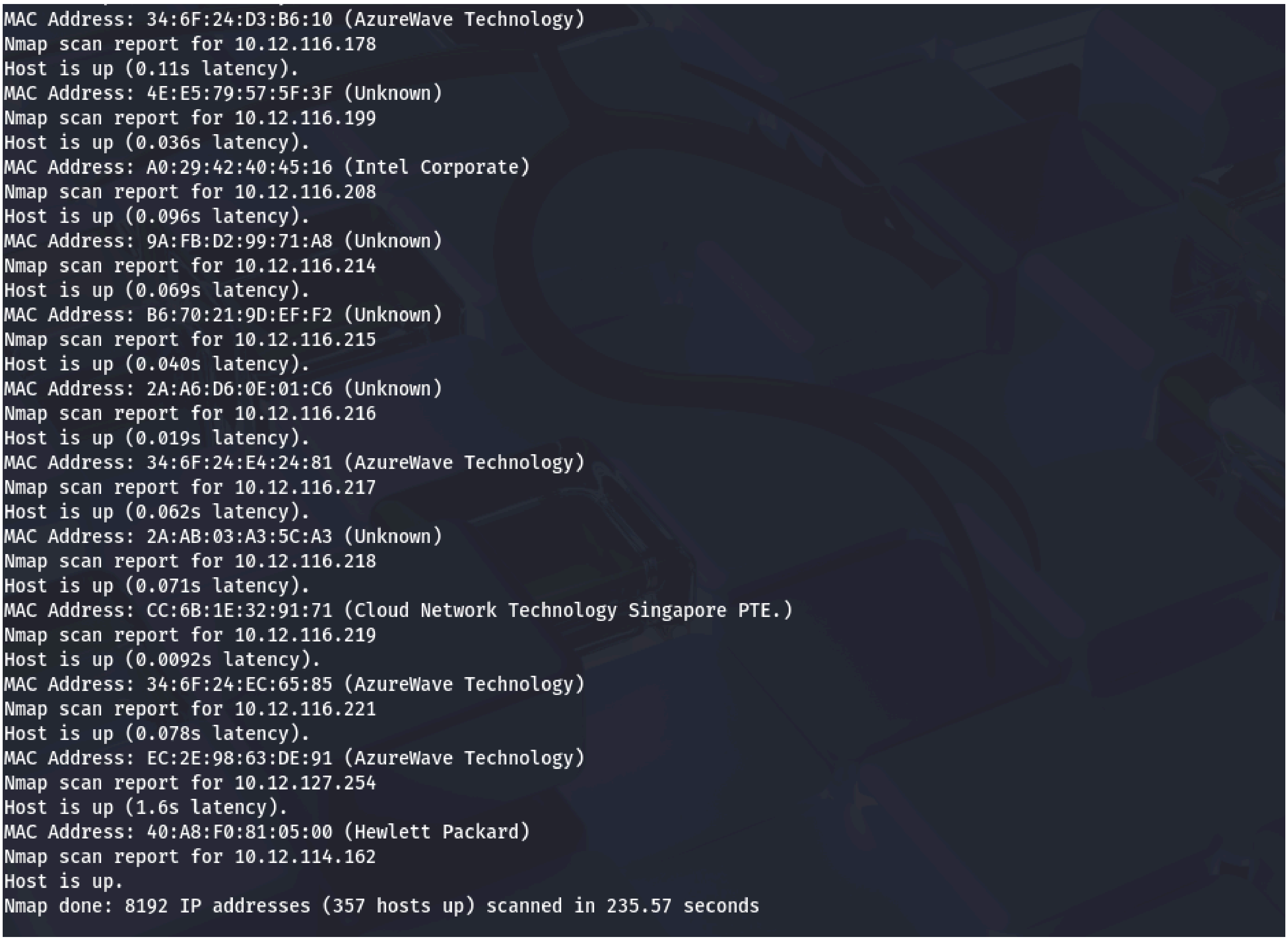
```
┌──(siddhu㉿siddhu)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:15:73:55 brd ff:ff:ff:ff:ff:ff
    inet 10.12.114.162/19 brd 10.12.127.255 scope global dynamic noprefixroute eth0
       valid_lft 691044sec preferred_lft 691044sec
    inet6 fe80::a00:27ff:fe15:7355/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(siddhu㉿siddhu)-[~]
└─$ █
```

10.12.114.162/19 is my ip address



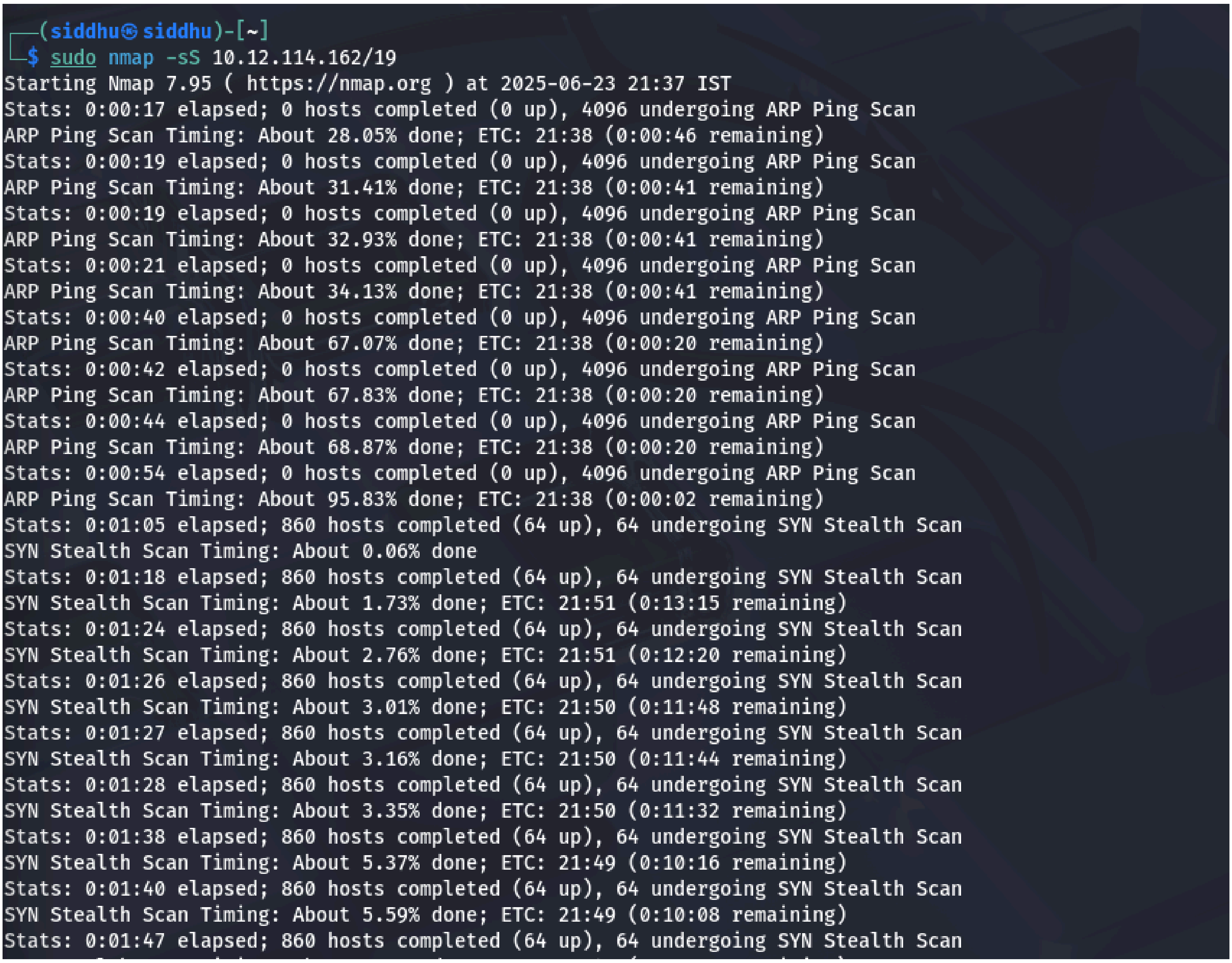
```
┌──(siddhu㉿siddhu)-[~]
└─$ sudo nmap -sn 10.12.114.162/19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:32 IST
Stats: 0:00:45 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 62.51% done; ETC: 21:33 (0:00:28 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 62.63% done; ETC: 21:33 (0:00:29 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 62.99% done; ETC: 21:34 (0:00:40 remaining)
Stats: 0:01:10 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 63.01% done; ETC: 21:34 (0:00:42 remaining)
Stats: 0:01:23 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 63.12% done; ETC: 21:34 (0:00:49 remaining)
Stats: 0:01:46 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 63.45% done; ETC: 21:35 (0:01:02 remaining)
Stats: 0:01:59 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 63.57% done; ETC: 21:35 (0:01:09 remaining)
Stats: 0:02:02 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 63.60% done; ETC: 21:35 (0:01:10 remaining)
Stats: 0:02:03 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 63.61% done; ETC: 21:35 (0:01:11 remaining)
Nmap scan report for 10.12.96.1
Host is up (0.0035s latency).
MAC Address: 00:00:5E:00:01:FE (Icann, Iana Department)
Nmap scan report for 10.12.96.11
Host is up (0.0030s latency).
MAC Address: 44:31:92:8F:64:A0 (Hewlett Packard)
Nmap scan report for 10.12.98.12
Host is up (0.082s latency).
MAC Address: A8:41:F4:25:59:E9 (AzureWave Technology)
Nmap scan report for 10.12.98.13
Host is up (0.070s latency).
MAC Address: 50:C2:E8:18:59:B3 (Cloud Network Technology Singapore PTE.)
```



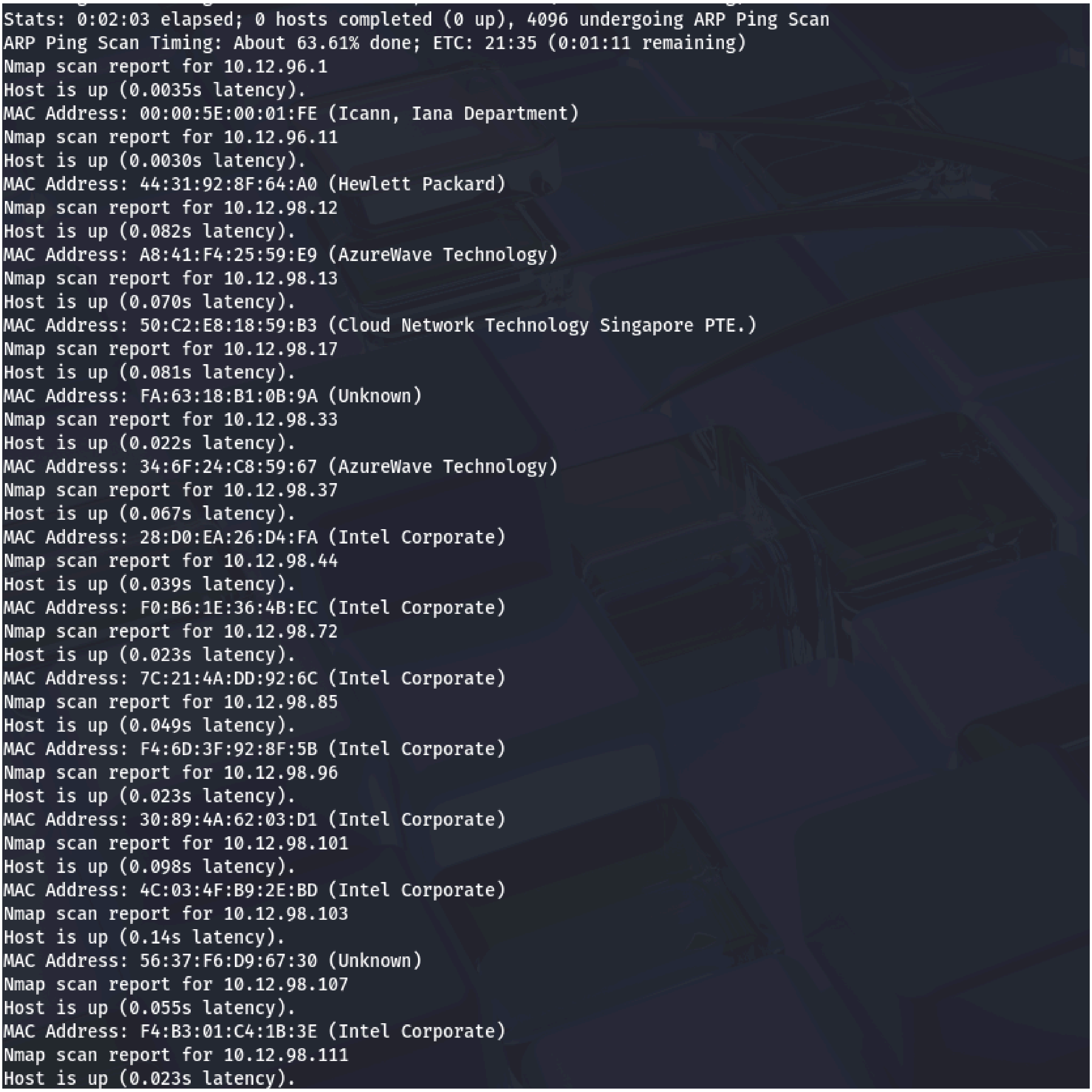
```
MAC Address: 34:6F:24:D3:B6:10 (AzureWave Technology)
Nmap scan report for 10.12.116.178
Host is up (0.11s latency).
MAC Address: 4E:E5:79:57:5F:3F (Unknown)
Nmap scan report for 10.12.116.199
Host is up (0.036s latency).
MAC Address: A0:29:42:40:45:16 (Intel Corporate)
Nmap scan report for 10.12.116.208
Host is up (0.096s latency).
MAC Address: 9A:FB:D2:99:71:A8 (Unknown)
Nmap scan report for 10.12.116.214
Host is up (0.069s latency).
MAC Address: B6:70:21:9D:EF:F2 (Unknown)
Nmap scan report for 10.12.116.215
Host is up (0.040s latency).
MAC Address: 2A:A6:D6:0E:01:C6 (Unknown)
Nmap scan report for 10.12.116.216
Host is up (0.019s latency).
MAC Address: 34:6F:24:E4:24:81 (AzureWave Technology)
Nmap scan report for 10.12.116.217
Host is up (0.062s latency).
MAC Address: 2A:AB:03:A3:5C:A3 (Unknown)
Nmap scan report for 10.12.116.218
Host is up (0.071s latency).
MAC Address: CC:6B:1E:32:91:71 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 10.12.116.219
Host is up (0.0092s latency).
MAC Address: 34:6F:24:EC:65:85 (AzureWave Technology)
Nmap scan report for 10.12.116.221
Host is up (0.078s latency).
MAC Address: EC:2E:98:63:DE:91 (AzureWave Technology)
Nmap scan report for 10.12.127.254
Host is up (1.6s latency).
MAC Address: 40:A8:F0:81:05:00 (Hewlett Packard)
Nmap scan report for 10.12.114.162
Host is up.
Nmap done: 8192 IP addresses (357 hosts up) scanned in 235.57 seconds
```

3.Run: nmap -sS 10.12.114.162/19 to perform TCP SYN scan

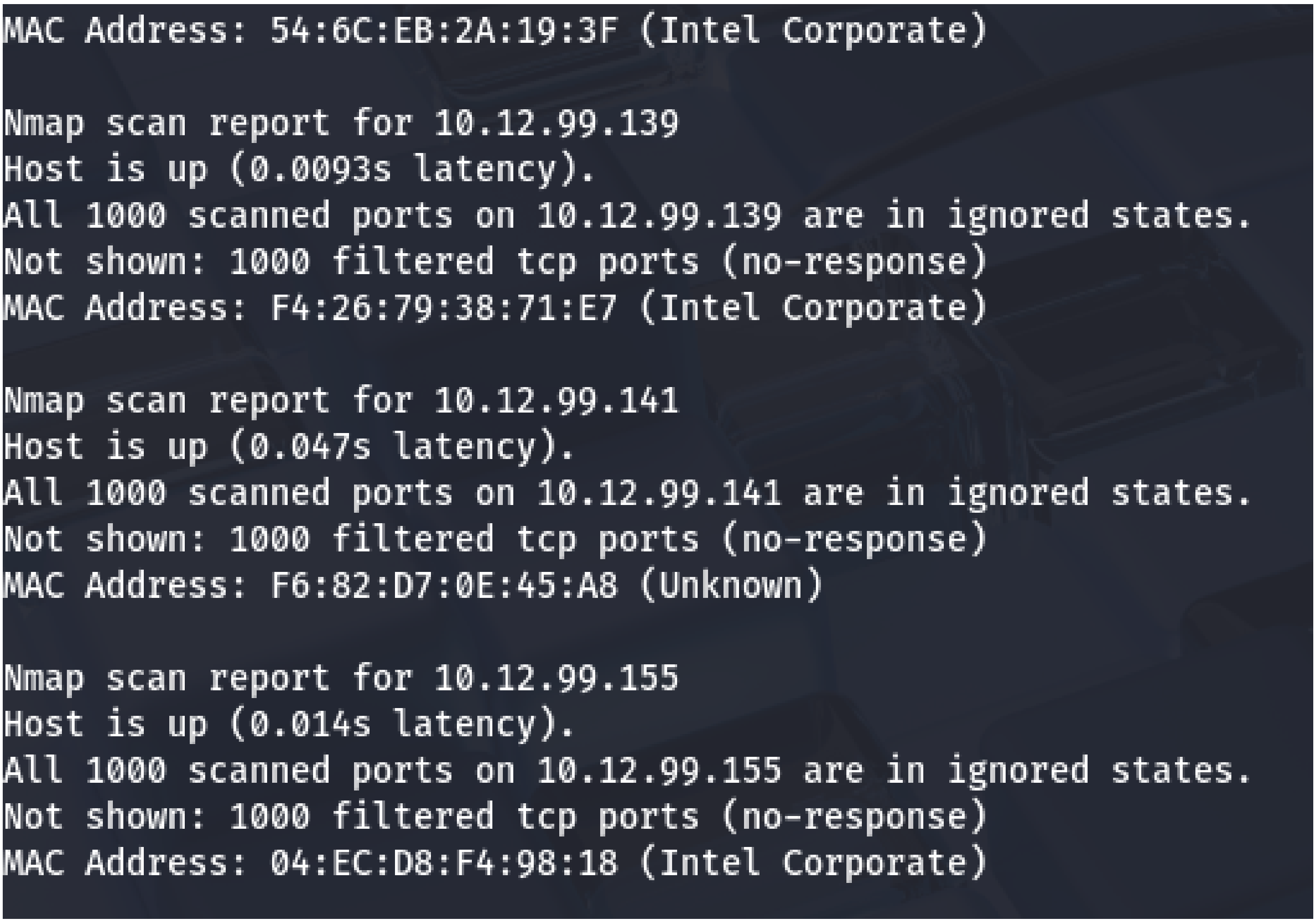
this result i got when i connected to campus wifi



```
┌──(siddhu㉿siddhu)-[~]
└─$ sudo nmap -sS 10.12.114.162/19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:37 IST
Stats: 0:00:17 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 28.05% done; ETC: 21:38 (0:00:46 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 31.41% done; ETC: 21:38 (0:00:41 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 32.93% done; ETC: 21:38 (0:00:41 remaining)
Stats: 0:00:21 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 34.13% done; ETC: 21:38 (0:00:41 remaining)
Stats: 0:00:40 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 67.07% done; ETC: 21:38 (0:00:20 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 67.83% done; ETC: 21:38 (0:00:20 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 68.87% done; ETC: 21:38 (0:00:20 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 95.83% done; ETC: 21:38 (0:00:02 remaining)
Stats: 0:01:05 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.06% done
Stats: 0:01:18 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.73% done; ETC: 21:51 (0:13:15 remaining)
Stats: 0:01:24 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.76% done; ETC: 21:51 (0:12:20 remaining)
Stats: 0:01:26 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.01% done; ETC: 21:50 (0:11:48 remaining)
Stats: 0:01:27 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.16% done; ETC: 21:50 (0:11:44 remaining)
Stats: 0:01:28 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.35% done; ETC: 21:50 (0:11:32 remaining)
Stats: 0:01:38 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.37% done; ETC: 21:49 (0:10:16 remaining)
Stats: 0:01:40 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.59% done; ETC: 21:49 (0:10:08 remaining)
Stats: 0:01:47 elapsed; 860 hosts completed (64 up), 64 undergoing SYN Stealth Scan
```



```
Stats: 0:02:03 elapsed; 0 hosts completed (0 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 63.61% done; ETC: 21:35 (0:01:11 remaining)
Nmap scan report for 10.12.96.1
Host is up (0.0035s latency).
MAC Address: 00:00:5E:00:01:FE (Icann, Iana Department)
Nmap scan report for 10.12.96.11
Host is up (0.0030s latency).
MAC Address: 44:31:92:8F:64:A0 (Hewlett Packard)
Nmap scan report for 10.12.98.12
Host is up (0.082s latency).
MAC Address: A8:41:F4:25:59:E9 (AzureWave Technology)
Nmap scan report for 10.12.98.13
Host is up (0.070s latency).
MAC Address: 50:C2:E8:18:59:B3 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 10.12.98.17
Host is up (0.081s latency).
MAC Address: FA:63:18:B1:0B:9A (Unknown)
Nmap scan report for 10.12.98.33
Host is up (0.022s latency).
MAC Address: 34:6F:24:C8:59:67 (AzureWave Technology)
Nmap scan report for 10.12.98.37
Host is up (0.067s latency).
MAC Address: 28:D0:EA:26:D4:FA (Intel Corporate)
Nmap scan report for 10.12.98.44
Host is up (0.039s latency).
MAC Address: F0:B6:1E:36:4B:EC (Intel Corporate)
Nmap scan report for 10.12.98.72
Host is up (0.023s latency).
MAC Address: 7C:21:4A:DD:92:6C (Intel Corporate)
Nmap scan report for 10.12.98.85
Host is up (0.049s latency).
MAC Address: F4:6D:3F:92:8F:5B (Intel Corporate)
Nmap scan report for 10.12.98.96
Host is up (0.023s latency).
MAC Address: 30:89:4A:62:03:D1 (Intel Corporate)
Nmap scan report for 10.12.98.101
Host is up (0.098s latency).
MAC Address: 4C:03:4F:B9:2E:BD (Intel Corporate)
Nmap scan report for 10.12.98.103
Host is up (0.14s latency).
MAC Address: 56:37:F6:D9:67:30 (Unknown)
Nmap scan report for 10.12.98.107
Host is up (0.055s latency).
MAC Address: F4:B3:01:C4:1B:3E (Intel Corporate)
Nmap scan report for 10.12.98.111
Host is up (0.023s latency).
```



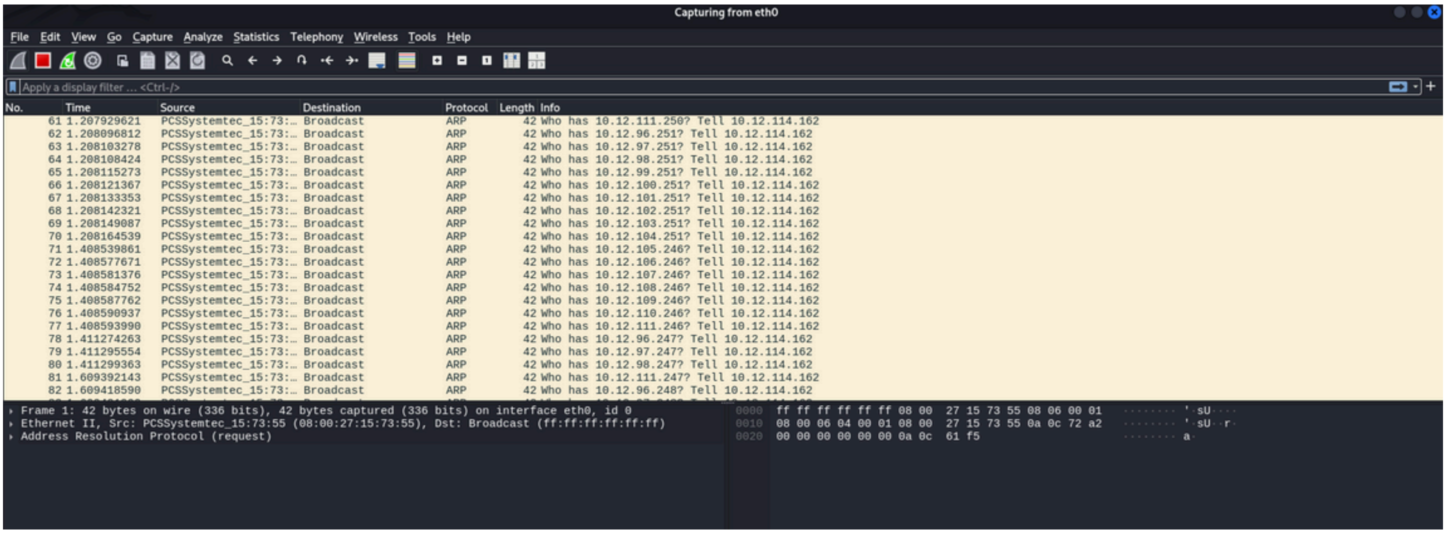
```
MAC Address: 54:6C:EB:2A:19:3F (Intel Corporate)

Nmap scan report for 10.12.99.139
Host is up (0.0093s latency).
All 1000 scanned ports on 10.12.99.139 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F4:26:79:38:71:E7 (Intel Corporate)

Nmap scan report for 10.12.99.141
Host is up (0.047s latency).
All 1000 scanned ports on 10.12.99.141 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F6:82:D7:0E:45:A8 (Unknown)

Nmap scan report for 10.12.99.155
Host is up (0.014s latency).
All 1000 scanned ports on 10.12.99.155 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 04:EC:D8:F4:98:18 (Intel Corporate)
```

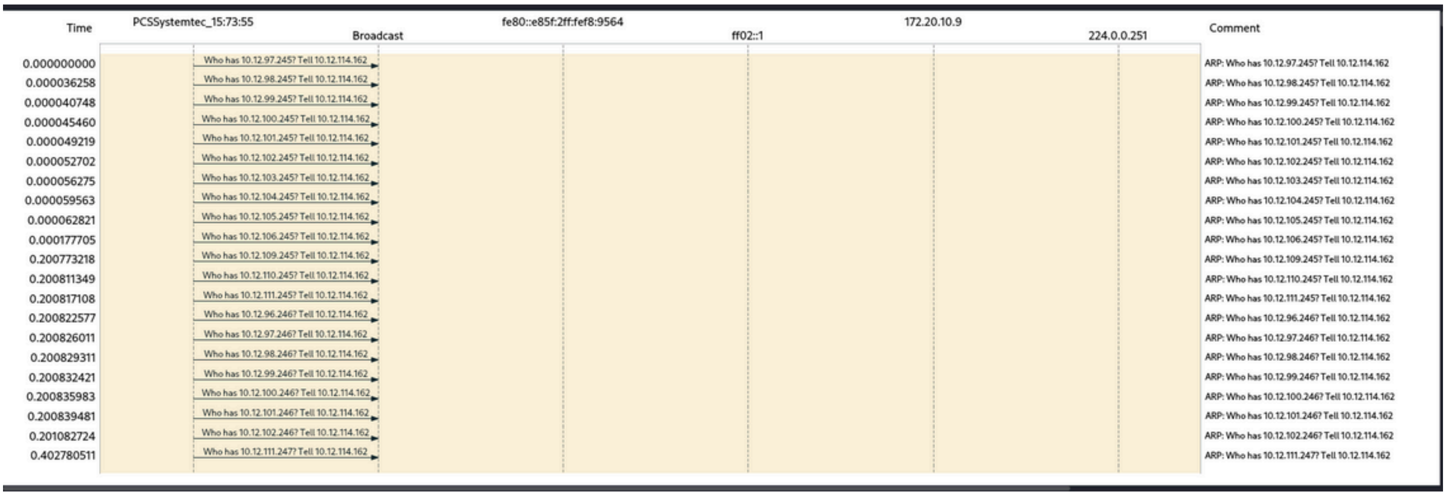
wireshark:


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source                  Destination   Protocol  Length Info
   61 1.207929621   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.111.250? Tell 10.12.114.162
   62 1.208096812   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.96.251? Tell 10.12.114.162
   63 1.208103278   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.97.251? Tell 10.12.114.162
   64 1.208108424   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.98.251? Tell 10.12.114.162
   65 1.208115273   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.99.251? Tell 10.12.114.162
   66 1.208121367   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.100.251? Tell 10.12.114.162
   67 1.208133353   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.101.251? Tell 10.12.114.162
   68 1.208142321   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.102.251? Tell 10.12.114.162
   69 1.208149087   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.103.251? Tell 10.12.114.162
   70 1.208164539   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.104.251? Tell 10.12.114.162
   71 1.408539861   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.105.246? Tell 10.12.114.162
   72 1.408577671   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.106.246? Tell 10.12.114.162
   73 1.408581376   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.107.246? Tell 10.12.114.162
   74 1.408584752   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.108.246? Tell 10.12.114.162
   75 1.408587762   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.109.246? Tell 10.12.114.162
   76 1.408590937   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.110.246? Tell 10.12.114.162
   77 1.408593990   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.111.246? Tell 10.12.114.162
   78 1.411274263   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.96.247? Tell 10.12.114.162
   79 1.411295554   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.97.247? Tell 10.12.114.162
   80 1.411299363   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.98.247? Tell 10.12.114.162
   81 1.609392143   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.111.247? Tell 10.12.114.162
   82 1.609418590   PCSSystemtec_15:73:...  Broadcast     ARP         42 Who has 10.12.96.248? Tell 10.12.114.162
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_15:73:55 (08:00:27:15:73:55), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 08 00  27 15 73 55 08 06 00 01   ········ '·sU····
0010  08 00 06 04 00 01 08 00  27 15 73 55 0a 0c 72 a2   ········ '·sU··r·
0020  00 00 00 00 00 00 0a 0c  61 f5                     ········ a·
```


PCSSystemtec_15:73:55
Broadcast
fe80::e85f:2ff:fef8:9564
ff02::1
172.20.10.9
224.0.0.251
Who has 10.12.97.245? Tell 10.12.114.162
Who has 10.12.98.245? Tell 10.12.114.162
Who has 10.12.99.245? Tell 10.12.114.162
Who has 10.12.100.245? Tell 10.12.114.162
Who has 10.12.101.245? Tell 10.12.114.162
Who has 10.12.102.245? Tell 10.12.114.162
Who has 10.12.103.245? Tell 10.12.114.162
Who has 10.12.104.245? Tell 10.12.114.162
Who has 10.12.105.245? Tell 10.12.114.162
Who has 10.12.106.245? Tell 10.12.114.162
Who has 10.12.109.245? Tell 10.12.114.162
Who has 10.12.110.245? Tell 10.12.114.162
Who has 10.12.111.245? Tell 10.12.114.162
Who has 10.12.96.246? Tell 10.12.114.162
Who has 10.12.97.246? Tell 10.12.114.162
Who has 10.12.98.246? Tell 10.12.114.162
Who has 10.12.99.246? Tell 10.12.114.162
Who has 10.12.100.246? Tell 10.12.114.162
Who has 10.12.101.246? Tell 10.12.114.162
Who has 10.12.102.246? Tell 10.12.114.162
Who has 10.12.111.247? Tell 10.12.114.162

```
Time          Comment
0.000000000   ARP: Who has 10.12.97.245? Tell 10.12.114.162
0.000036258   ARP: Who has 10.12.98.245? Tell 10.12.114.162
0.000040748   ARP: Who has 10.12.99.245? Tell 10.12.114.162
0.000045460   ARP: Who has 10.12.100.245? Tell 10.12.114.162
0.000049219   ARP: Who has 10.12.101.245? Tell 10.12.114.162
0.000052702   ARP: Who has 10.12.102.245? Tell 10.12.114.162
0.000056275   ARP: Who has 10.12.103.245? Tell 10.12.114.162
0.000059563   ARP: Who has 10.12.104.245? Tell 10.12.114.162
0.000062821   ARP: Who has 10.12.105.245? Tell 10.12.114.162
0.000177705   ARP: Who has 10.12.106.245? Tell 10.12.114.162
0.200773218   ARP: Who has 10.12.109.245? Tell 10.12.114.162
0.200811349   ARP: Who has 10.12.110.245? Tell 10.12.114.162
0.200817108   ARP: Who has 10.12.111.245? Tell 10.12.114.162
0.200822577   ARP: Who has 10.12.96.246? Tell 10.12.114.162
0.200826011   ARP: Who has 10.12.97.246? Tell 10.12.114.162
0.200829311   ARP: Who has 10.12.98.246? Tell 10.12.114.162
0.200832421   ARP: Who has 10.12.99.246? Tell 10.12.114.162
0.200835983   ARP: Who has 10.12.100.246? Tell 10.12.114.162
0.200839481   ARP: Who has 10.12.101.246? Tell 10.12.114.162
0.201082724   ARP: Who has 10.12.102.246? Tell 10.12.114.162
0.402780511   ARP: Who has 10.12.111.247? Tell 10.12.114.162
```

6.Research common services running on those ports.

1. **6. Purpose of Common Open Ports**
2. **135/tcp (MSRPC):**
   - Enables communication between Windows applications and services over a network.
   - Commonly used by the Windows Remote Procedure Call (RPC) service.
3. **445/tcp (Microsoft-DS / SMB):**
   - Supports file sharing, printer sharing, and access to shared network resources on Windows systems.
   - Used by the Server Message Block (SMB) protocol.
4. **3306/tcp (MySQL):**
   - Handles connections to MySQL databases.
   - Used for querying, updating, and managing structured data in relational databases.
5. **53/tcp (DNS):**
   - Resolves domain names into IP addresses (DNS resolution).
   - Also supports DNS zone transfers and large queries over TCP.

**7. Identify Potential Security Risks from Open Ports**

1. **135/tcp (MSRPC):**
   - Frequently targeted for Windows exploits and vulnerabilities.
   - Can be used for remote code execution or lateral movement within a network.
2. **445/tcp (Microsoft-DS / SMB):**
   - Commonly used in ransomware attacks (e.g., WannaCry).
   - Enables unauthorized file access, data exposure, and remote code execution if misconfigured.
3. **3306/tcp (MySQL):**
   - Exposes databases to brute-force or SQL injection attacks.
   - May lead to sensitive data leaks if not properly secured or patched.
4. **53/tcp (DNS):**
   - Can be exploited for DNS tunneling and data exfiltration.
   - Vulnerable to spoofing, cache poisoning, or other attacks if misconfigured